(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－259621
（P2002－259621A）
(43)公開日　平成14年９月13日(2002.9.13)

(51)Int.Cl.⁷	識別記号	ＦＩ		ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　17/60	１４８	Ｇ０６Ｆ　17/60	１４８	５Ｊ１０４
	１５４		１５４	
	５０２		５０２	
	５１０		５１０	
	５１２		５１２	

審査請求　未請求　請求項の数11　ＯＬ　（全　８　頁）　最終頁に続く

(21)出願番号　特願2001－52429(P2001－52429)

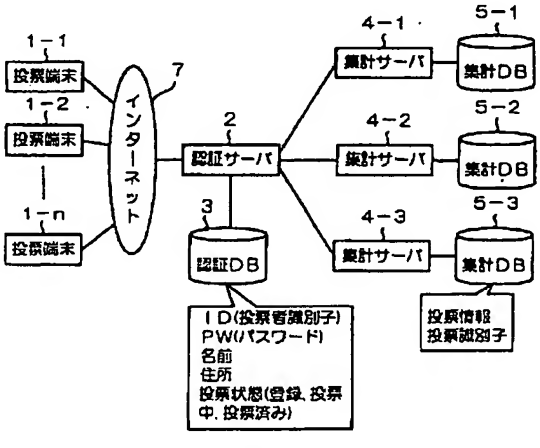
(22)出願日　平成13年２月27日(2001.2.27)

(71)出願人　000102739
エヌ・ティ・ティ・アドバンステクノロジ株式会社
東京都新宿区西新宿二丁目１番１号
(72)発明者　田中　利清
東京都新宿区西新宿二丁目１番１号　エヌ・ティ・ティ・アドバンステクノロジ株式会社内
(74)代理人　100064908
弁理士　志賀　正武

Ｆターム(参考)　5J104 AA07 AA09 AA16 EA06 EA19
KA01 LA08 MA01 NA05 NA35
NA41 PA17

(54)【発明の名称】　電子投票システムおよび電子投票方法

(57)【要約】
【課題】　人手の削減、開票スペースの縮小、無効票や疑問票の根絶、集計ミスの防止を実現する。
【解決手段】　投票端末１－１～１－ｎでは、投票者がタッチパネルを用いて投票する。認証サーバ２は、投票情報にブラインド署名を生成することで、投票者を認証する。投票端末１－１～１－ｎは、投票情報を暗号化技術により、２重の電子的封筒で密封してインターネット７を介して認証サーバ２に送る。認証サーバ２は、外側の封筒を開封し、３つの集計サーバ４－１～４－３へ送る。集計サーバ４－１～４－３は、各々、内側の封筒を開封し、投票内容に基づいて集計を行う。開票終了後、集計サーバ４－１～４－３が集票・集計した投票結果を照合し、不一致が見つかった場合には、多数決で正解値を決める。



1

【特許請求の範囲】

【請求項１】　ネットワークに接続され、投票者により候補者に対して行われる投票内容を暗号化し、暗号化投票内容を生成する投票端末と、

前記投票端末における前記投票者を、前記ネットワークを介して認証する認証装置と、

前記認証装置を介して前記投票端末からの暗号化投票内容を復号して投票内容を取得し、該投票内容に基づいて候補者の得票を集計する集計装置とを具備することを特徴とする電子投票システム。

【請求項２】　前記投票端末は、

投票者により行われた投票内容を暗号化して、第１の暗号化投票内容を生成する第１の暗号化手段と、

前記第１の暗号化手段により暗号化された第１の暗号化投票内容を暗号化して第２の暗号化投票内容を生成する第２の暗号化手段とを具備し、

前記認証装置は、

前記投票端末の前記第２の暗号化手段により暗号化された第２の暗号化投票内容を復号して前記第１の暗号化投票内容を取得する第１の復号化手段を具備し、前記集計装置は、

前記認証装置の前記第１の復号化手段により復号された第１の暗号化投票内容を復号して前記投票内容を取得する第２の復号化手段を具備することを特徴とする請求項１記載の電子投票システム。

【請求項３】　前記第１の暗号化手段は、

投票者により行われた投票内容を、第１の共通鍵を用いて暗号化し、該第１の共通鍵を、前記集計装置の第１の公開鍵を用いて暗号化し、

前記第２の暗号化手段は、

前記第１の暗号化投票内容を、第２の共通鍵を用いて暗号化し、該第２の共通鍵を、前記認証装置の第２の公開鍵を用いて暗号化し、

前記第１の復号化手段は、暗号化された第２の共通鍵を、前記第２の公開鍵に対応する第２の秘密鍵を用いて復号して前記第２の共通鍵を取得する第２の共通鍵復号手段と、復号された第２の共通鍵を用いて、前記第２の暗号化投票内容を復号して前記第１の暗号化投票内容を取得する第２の暗号化投票内容復号化手段とを備え、

前記第２の復号化手段は、暗号化された第１の共通鍵を、前記第１の公開鍵に対応する第１の秘密鍵を用いて復号して前記第１の共通鍵を取得する第１の共通鍵復号手段と、復号された第１の共通鍵を用いて、前記第１の暗号化投票内容を復号して前記投票内容を取得する第１の暗号化投票内容復号化手段とを備えることを特徴とする請求項２記載の電子投票システム。

【請求項４】　前記認証装置は、

投票者の正当性を認証すべく、前記投票端末により暗号化された投票内容に対してブラインド署名を生成するブラインド署名手段を備え、

2

前記投票端末は、

投票者により選択された候補者に対応する投票内容を暗号化し、前記認証装置に送信する第３の暗号化手段と、

前記認証装置のブラインド署名手段により生成されたブラインド署名から署名情報を取得する署名取得手段とを備えることを特徴とする請求項１ないし３のいずれかの記載の電子投票システム。

【請求項５】　前記集計装置は、

前記投票内容に対して識別情報を生成する識別情報生成手段と、

前記投票内容を前記識別情報とともに蓄積する蓄積手段とを具備することを特徴とする請求項１ないし４のいずれかの記載の電子投票システム。

【請求項６】　前記第１の公開鍵および第１の秘密鍵、ならびに前記第２の公開鍵および第２の秘密鍵は、各々、前記認証装置または前記集計装置に着脱可能な、外部へ情報が漏洩しないようにプロテクトされた、ＩＣカード内で生成・管理されることを特徴とする請求項３ないし５のいずれかの記載の電子投票システム。

【請求項７】　ネットワークに接続された投票端末から投票者が投票し、

該投票された投票内容を暗号化して、前記ネットワークに接続された認証装置に送信し、

前記認証装置は、投票者の認証を行い、認証された場合は、前記暗号化された内容を前記集計装置に送信し、

前記集計装置によって前記暗号化投票内容を復号して投票内容を取得し、

該投票内容に基づいて候補者の得票を集計することを特徴とする電子投票方法。

【請求項８】　前記投票端末は、前記投票内容を暗号化して暗号化投票内容を生成し、

前記認証装置は、前記投票端末により暗号化された暗号化投票内容に対してブラインド署名を生成し、

前記投票端末は、前記ブラインド署名から署名情報を取得することを特徴とする請求項７記載の電子投票方法。

【請求項９】　前記投票内容の暗号化では、

前記投票者により行われた投票内容を、第１の共通鍵を用いて暗号化して前記第１の暗号化投票内容を生成し、

前記第１の共通鍵を、前記集計装置の第１の公開鍵を用いて暗号化し、

前記第１の暗号化投票内容を、第２の共通鍵を用いて暗号化して第２の暗号化投票内容を生成し、

前記第２の共通鍵を、前記認証装置の第２の公開鍵を用いて暗号化し、

前記暗号化投票内容の復号化では、

前記暗号化された第２の共通鍵を、前記第２の公開鍵に対応する第２の秘密鍵を用いて復号して前記第２の共通鍵を取得し、

前記復号された第２の共通鍵を用いて、前記第２の暗号化投票内容を復号して前記第１の暗号化投票内容を取得

し、
前記暗号化された第１の共通鍵を、前記第１の公開鍵に対応する第１の秘密鍵を用いて復号して前記第１の共通鍵を取得し、
前記復号された第１の共通鍵を用いて、前記第１の暗号化投票内容を復号して投票内容を取得することを特徴とする請求項７記載の電子投票方法。
【請求項１０】　前記投票内容に対して識別情報を生成し、前記投票内容を前記識別情報とともに蓄積することを特徴とする請求項７ないし９のいずれかに記載の電子投票方法。
【請求項１１】　前記第１の公開鍵および第１の秘密鍵、ならびに前記第２の公開鍵および第２の秘密鍵は、各々、認証装置または集計装置に着脱可能な、外部へ情報が漏洩しないようにプロテクトされた、ＩＣカード内で生成・管理されることを特徴とする請求項７ないし１０のいずれかに記載の電子投票方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、国政選挙や地方選挙などの投票に用いて好適な電子投票システムおよび電子投票方法に関する。
【０００２】
【従来の技術】従来より、国政選挙や地方選挙などの投票においては、有権者が投票所で、投票用紙に候補者氏名を書き込み、該投票用紙を集め、多くの人手で１枚ずつ投票用紙に書かれた候補者氏名を確認、カウントすることで行われてきた。
【０００３】
【発明が解決しようとする課題】しかしながら、上述した従来技術では、大量の人手や、開票スペースが必要である。また、投票者氏名は、投票者による手書きであるため、記入ミスによる無効票や疑問票が絶えない。また、人による目視確認であるため、集計ミスも起り得るという問題があった。
【０００４】この発明は上述した事情に鑑みてなされたもので、人手の削減、開票スペースの縮小、無効票や疑問票の根絶、集計ミスの防止を実現することができる電子投票システムおよび電子投票方法を提供することを目的とする。
【０００５】
【課題を解決するための手段】上述した問題点を解決するために、請求項１記載の発明では、ネットワークに接続され、投票者により候補者に対して行われる投票内容を暗号化し、暗号化投票内容を生成する投票端末と、前記投票端末における前記投票者を、前記ネットワークを介して認証する認証装置と、前記認証装置を介して前記投票端末からの暗号化投票内容を復号して投票内容を取得し、該投票内容に基づいて候補者の得票を集計する集計装置とを具備することを特徴とする。
【０００６】また、請求項２記載の発明では、請求項１記載の電子投票システムにおいて、前記投票端末は、投票者により行われた投票内容を暗号化して、第１の暗号化投票内容を生成する第１の暗号化手段と、前記第１の暗号化手段により暗号化された第１の暗号化投票内容を暗号化して第２の暗号化投票内容を生成する第２の暗号化手段とを具備し、前記認証装置は、前記投票端末の前記第２の暗号化手段により暗号化された第２の暗号化投票内容を復号して前記第１の暗号化投票内容を取得する第１の復号化手段を具備し、前記集計装置は、前記認証装置の前記第１の復号化手段により復号された第１の暗号化投票内容を復号して前記投票内容を取得する第２の復号化手段を具備することを特徴とする。
【０００７】また、請求項３記載の発明では、請求項２記載の電子投票システムにおいて、前記第１の暗号化手段は、投票者により行われた投票内容を、第１の共通鍵を用いて暗号化し、該第１の共通鍵を、前記集計装置の第１の公開鍵を用いて暗号化し、前記第２の暗号化手段は、前記第１の暗号化投票内容を、第２の共通鍵を用いて暗号化し、該第２の共通鍵を、前記認証装置の第２の公開鍵を用いて暗号化し、前記第１の復号化手段は、暗号化された第２の共通鍵を、前記第２の公開鍵に対応する第２の秘密鍵を用いて復号して前記第２の共通鍵を取得する第２の共通鍵復号手段と、復号された第２の共通鍵を用いて、前記第２の暗号化投票内容を復号して前記第１の暗号化投票内容を取得する第２の暗号化投票内容復号化手段とを備え、前記第２の復号化手段は、暗号化された第１の共通鍵を、前記第１の公開鍵に対応する第１の秘密鍵を用いて復号して前記第１の共通鍵を取得する第１の共通鍵復号手段と、復号された第１の共通鍵を用いて、前記第１の暗号化投票内容を復号して前記投票内容を取得する第１の暗号化投票内容復号化手段とを備えることを特徴とする。
【０００８】また、請求項４記載の発明では、請求項１ないし３のいずれかの記載の電子投票システムにおいて、前記認証装置は、投票者の正当性を認証すべく、前記投票端末により暗号化された投票内容に対してブラインド署名を生成するブラインド署名手段を備え、前記投票端末は、投票者により選択された候補者に対応する投票内容を暗号化し、前記認証装置に送信する第３の暗号化手段と、前記認証装置のブラインド署名手段により生成されたブラインド署名から署名情報を取得する署名取得手段とを備えることを特徴とする。
【０００９】また、請求項５記載の発明では、請求項１ないし４のいずれかの記載の電子投票システムにおいて、前記集計装置は、前記投票内容に対して識別情報を生成する識別情報生成手段と、前記投票内容を前記識別情報とともに蓄積する蓄積手段とを具備することを特徴とする。
【００１０】また、請求項６記載の発明では、請求項３

ないし５のいずれかの記載の電子投票システムにおいて、前記第１の公開鍵および第１の秘密鍵、ならびに前記第２の公開鍵および第２の秘密鍵は、各々、前記認証装置または前記集計装置に着脱可能な、外部へ情報が漏洩しないようにプロテクトされた、ＩＣカード内で生成・管理されることを特徴とする。

【００１１】上述した問題点を解決するために、請求項７記載の発明では、ネットワークに接続された投票端末から投票者が投票し、該投票された投票内容を暗号化して、前記ネットワークに接続された認証装置に送信し、前記認証装置は、投票者の認証を行い、認証された場合は、前記暗号化された内容を前記集計装置に送信し、前記集計装置によって前記暗号化投票内容を復号して投票内容を取得し、該投票内容に基づいて候補者の得票を集計することを特徴とする。

【００１２】また、請求項８記載の発明では、請求項７記載の電子投票方法において、前記投票端末は、前記投票内容を暗号化して暗号化投票内容を生成し、前記認証装置は、前記投票端末により暗号化された暗号化投票内容に対してブラインド署名を生成し、前記投票端末は、前記ブラインド署名から署名情報を取得することを特徴とする。

【００１３】また、請求項９記載の発明では、請求項７記載の電子投票方法において、前記投票内容の暗号化では、前記投票者により行われた投票内容を、第１の共通鍵を用いて暗号化して前記第１の暗号化投票内容を生成し、前記第１の共通鍵を、前記集計装置の第１の公開鍵を用いて暗号化し、前記第１の暗号化投票内容を、第２の共通鍵を用いて暗号化して第２の暗号化投票内容を生成し、前記第２の共通鍵を、前記認証装置の第２の公開鍵を用いて暗号化し、前記暗号化投票内容の復号化では、前記暗号化された第２の共通鍵を、前記第２の公開鍵に対応する第２の秘密鍵を用いて復号して前記第２の共通鍵を取得し、前記復号された第２の共通鍵を用いて、前記第２の暗号化投票内容を復号して前記第１の暗号化投票内容を取得し、前記暗号化された第１の共通鍵を、前記第１の公開鍵に対応する第１の秘密鍵を用いて復号して前記第１の共通鍵を取得し、前記復号された第１の共通鍵を用いて、前記第１の暗号化投票内容を復号して投票内容を取得することを特徴とする。

【００１４】また、請求項１０記載の発明では、請求項７ないし９のいずれかに記載の電子投票方法において、前記投票内容に対して識別情報を生成し、前記投票内容を前記識別情報とともに蓄積することを特徴とする。

【００１５】また、請求項１１記載の発明では、請求項７ないし１０のいずれかに記載の電子投票方法において、前記第１の公開鍵および第１の秘密鍵、ならびに前記第２の公開鍵および第２の秘密鍵は、各々、認証装置または集計装置に着脱可能な、外部へ情報が漏洩しないようにプロテクトされた、ＩＣカード内で生成・管理されることを特徴とする。

【００１６】この発明では、ネットワークに接続された投票端末から投票者が投票し、該投票された投票内容を、前記ネットワークに接続された認証装置により認証し、前記認証された投票内容を暗号化して、前記ネットワークを介して、前記認証装置に接続されている集計装置に送信し、前記集計装置によって前記暗号化投票内容を復号して投票内容を取得し、該投票内容に基づいて候補者の得票を集計する。したがって、人手の削減、開票スペースの縮小、無効票や疑問票の根絶、集計ミスの防止を実現することが可能となる。

【００１７】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態を説明する。

Ａ．実施形態の構成

図１は、本発明の実施形態による電子投票システムの構成を示すブロック図である。図１において、投票端末１－１，１－２，…，１－ｎは、投票所に設置された端末であり、パーソナルコンピュータなどから構成されている。該投票端末１－１～１－ｎは、インターネット７に接続されている。投票端末１－１～１－ｎは、１つの投票所に複数台（ｎ台）設置されており、その設置台数は、投票所で投票する有権者の数に応じて定められている。

【００１８】上記投票端末１－１～１－ｎは、候補者情報を暗号化する機能、後述する認証サーバ２により生成されたディジタル署名を復号する機能（アンブラインド）、さらに、候補者情報とディジタル署名とに対して２重の暗号化を行う機能などを有する。これら機能（動作）については後述する。

【００１９】投票者は、投票端末１－１～１－ｎのタッチパネル上の数字ボタンをタッチすることで、投票者を認証するためのＩＤ（投票者識別子）やパスワード、候補者などを入力する。ＩＤ、パスワードは、例えば、図２に示すように、３桁毎のグループに分割し、各グループに番号を付ける。ＩＤ、パスワードは、高齢者等の投票者に考慮し、読み間違い、入力ミスを低減するために数字のみで構成することが好ましい。

【００２０】なお、投票端末１－１～１－ｎは、投票者の自宅に設置されてもよいが、この場合、所定の投票用ソフトウエアを予めインストールしておく必要がある。

【００２１】認証サーバ２は、インターネット７を介して投票端末１－１～１－ｎに対して、上記ＩＤ、パスワード、誕生日などを要求し、それら情報を照合して投票者を認証する。また、認証サーバ２は、インターネット７を介して投票端末１－１～１－ｎに対して、候補者情報（氏名、党名、顔写真）を送信し、投票端末１－１～１－ｎからの投票情報（暗号化済）にディジタル署名（ブラインド署名）を発行する。また、認証サーバ２は、投票端末１－１～１－ｎからの暗号化された投票情

報を、後述する３台の集計サーバ４－１，４－２，４－３に送信するようになっている。また、認証サーバ２は、投票者の認証を行ったり、投票状態を管理したりするための認証データベース３を備えている。該認証データベース３は、投票者毎のＩＤ、パスワード、名前、住所、投票状態（登録、投票中、投票済み）を蓄積している。

【００２２】集計サーバ４－１～４－３は、それぞれが物理的に隔離され、同一の機能を有する３つのサーバからなる。集計サーバ４－１～４－３は、各々、それぞれ独立に集票および集計を行う。より具体的には、集計サーバ４－１～４－３は、各々、認証サーバ２からの投票情報に対して、認証サーバ２によるディジタル署名を検証し、投票識別子を生成・付加し、集計データベース５－１，５－２，５－３に格納する。それぞれの集計サーバ４－１～４－３による集計結果は、互いに照合され、不一致が見つかった場合には、多数決で正解値を決めるようになっている。

【００２３】なお、上述した認証サーバ２および集計サーバ４－１～４－３では、投票情報の暗号化と復号およびディジタル署名を行うようになっているが、該暗号化と復号およびディジタル署名において用いられる、秘密鍵の生成と復号、および署名生成は、ＩＣカードなどの記憶媒体内で実施されるようになっている。秘密鍵は、ＩＣカードから読み出せないようにプロテクトされている。このため、紛失等に対応したバックアップができないので、秘密鍵の種類の数（この例では２、集計サーバの場合には３種類）だけ署名および暗号化を行い、冗長化している。

【００２４】Ｂ．実施形態の動作次に、図３に示すフローチャートを参照して本実施形態の動作について詳細に説明する。ここで、図４は、認証サーバからディジタル署名を得る過程を示すフローチャートである。また、図５は、上記投票端末での密封、認証サーバでの開封、集計サーバでの開封の様子を示す概念図である。

【００２５】投票者は、予め自宅の端末からインターネットを介して認証サーバにアクセスし、認証サーバが提示する選挙管理Ｗｅｂ画面から個人情報（名前、住所など）を登録する（ステップＳ１）。認証サーバ２は、登録した投票者に対してＩＤ（投票者識別子）、ＰＷ（パスワード）が記入されたシール付きはがき（投票整理券）を自宅に郵送する（ステップＳ２）。なお、自宅に端末を所持しない有権者も居るので、現行通り、認証サーバ２（所轄役所）側から自動的に有権者に対してシール付きはがき（投票整理券）を自宅に郵送するようにしてもよい。

【００２６】次に、投票日になると、投票者は自宅の端末から投票を行う。自宅に端末を持たない投票者は自宅に郵送された投票整理券を持参して投票所に出向き、投票所の端末から投票を行う。投票者は、自宅又は投票所に設置された、投票端末１－ｉ（ｉ＝１～ｎ）から投票を開始する（ステップＳ３）。

【００２７】認証サーバ２は、インターネット７を介して、上記投票端末１－ｉに対してＩＤ、パスワードおよび誕生日の入力を要求する（ステップＳ４）。投票者は、投票端末１－ｉのタッチパネルから、自宅に郵送されたシール付きはがきに印字されたＩＤ、パスワード、および誕生日（ＭＭＤＤ）を入力する（ステップＳ５）。ＩＤ、パスワードは、インターネット７を介して認証サーバ２に送信される。

【００２８】認証サーバ２は、上記投票端末１－ｉから入力された、ＩＤ、パスワード、および誕生日を、認証データベース３の情報と照合し、正しい投票者であるか、すなわち有権者であるか、二重投票ではないかなどをチェックする（ステップＳ６）。投票者が正当と認証された場合は、認証サーバ２は、候補者情報（氏名、党名、顔写真など）を、インターネット７を介して上記投票端末１－ｉに送信する（ステップＳ７）。投票者が正当と認証されなかった場合は、その旨を投票端末１－ｉに表示し、当該投票者への処理を中止する。

【００２９】投票者は、投票端末１－ｉに表示される候補者情報を確認して候補者を選択（投票）する（ステップＳ８）。投票端末１－ｉでは、図４に示すように、選択された候補者の情報（以下、投票情報）をブラインド（暗号化）し、インターネット７を介して認証サーバ２に送信する（ステップＳ９）。認証サーバ２では、図４に示すように、上記暗号化された投票情報に対してディジタル署名（ブラインド署名）を生成し、インターネット７を介して、投票端末１－ｉに送信する（ステップＳ１０）。投票端末１－ｉでは、図４に示すように、上記ブラインド署名をアンブラインド（復号）し、ディジタル署名を取得する（ステップＳ１１）。このように、ブラインド署名を用いることで、認証サーバ２では、投票者を特定できるが、投票内容を知ることはできない（匿名性の保証）。そして、認証サーバにより、その投票者が本人であること、その投票内容が投票者本人によるものであること、票が重複して投じられていないことが認証されることになる。

【００３０】次にブラインド署名の方式の例を示す。認証サーバの秘密鍵をｄ、公開鍵をｅ、ｎ、投票情報をｍとする。また以下の演算はｎの剰余の基での演算である。投票端末は、乱数ｒを生成し、ｒのｅ乗とｍの積をｘとして認証サーバへ送付する。認証サーバはｘのｄ乗をｙとして投票端末へ送付する。このｙがブラインド署名である。投票端末はｙをｒで除算する。ｄ＝１／ｅであるので、除算結果はｍのｄ乗となり、これはｍに対する署名そのものである。

【００３１】次に、投票端末１－ｉでは、図５に示すように、上記投票情報（ディジタル署名を含む）を封筒Ａにより密封した後（ステップＳ１２）；さらに、封筒Ｂ

により密封し（ステップＳ１３）、インターネット７を介して認証サーバ２へ送信する。認証サーバ２では、図５に示すように、外側の封筒Ｂのみを開封し（ステップＳ１４）、集計サーバ４－１～４－３に送信する。集計サーバ４－１～４－３では、図５に示すように、封筒Ａを開封し（ステップＳ１５）、元の投票情報（ディジタル署名を含む）を取得する。

【００３２】以下に、上記投票端末１－１～１－ｎでの密封、認証サーバ２での開封、集計サーバ４－１～４－３での開封についてより詳細に説明する。ここで、図６は、上記投票端末での密封の詳細な様子を示す概念図である。また、図７は、上記認証サーバおよび集計サーバでの開封の詳細な様子を示す概念図である。

【００３３】投票端末１－１～１－ｎでは、図６に示すように、上記投票情報（ディジタル署名を含む）を共通鍵ＫＡ１で暗号化することにより（ステップＳａ１）、封筒Ａにより密封した後、上記共通鍵ＫＡ１を、集計サーバ４－ｉ（ｉ＝１，２，３）が公開している公開鍵ＫＢ１により暗号化する（ステップＳａ２）。次に、暗号化した投票情報（封筒Ａ）を、さらに、共通鍵ＫＡ２で暗号化することにより（ステップＳａ３）、封筒Ｂにより密封した後、上記共通鍵ＫＡ２を、認証サーバ２が公開している公開鍵ＫＢ２により暗号化する（ステップＳａ４）。これにより、投票情報は、封筒Ａ（内側）と封筒Ｂ（外側）で二重に密封（暗号化）されたことになる。該二重に暗号化された投票情報は、インターネット７を介して認証サーバ２へ送信される。

【００３４】認証サーバ２では、図７（ａ）に示すように、上記公開鍵ＫＢ２に対応する秘密鍵ＫＣ２により、暗号化された共通鍵ＫＡ２を復号して上記共通鍵ＫＡ２を取得し（ステップＳｂ１）、該共通鍵ＫＡ２で、上記二重に暗号化された投票情報（内側：封筒Ａ、外側：封筒Ｂ）を復号することで、外側の封筒Ｂを開封する（ステップＳｂ２）。そして、封筒Ａで密封された投票情報を集計サーバ４－１～４－３に送信する。

【００３５】集計サーバ４－ｉ（ｉ＝１，２，３）では、図７（ｂ）に示すように、上記公開鍵ＫＢ１に対応する秘密鍵ＫＣ１により、暗号化された共通鍵ＫＡ１を復号して共通鍵ＫＡ１を取得し（ステップＳｃ１）、該共通鍵ＫＡ１で、上記投票情報（封筒Ａ）を復号することで、封筒Ａを開封する（ステップＳｃ２）。この時点で、集計サーバ４－ｉには、元の投票情報（ディジタル署名を含む）が取得される。

【００３６】なお、上述した説明において、本実施形態では、３つの集計サーバ４－１～４－３を用いているので、実際には、集計サーバ毎に、それぞれの秘密鍵ＫＣ１－１，ＫＣ１－２，ＫＣ１－３と、該秘密鍵に対応する公開鍵ＫＢ１－１，ＫＢ１－２，ＫＢ１－３とを生成している。そして、投票端末１－ｉにおいて、投票情報を封筒Ａで密封する際には、共通鍵ＫＡ１を、上記公開鍵ＫＢ１－１，ＫＢ１－２，ＫＢ１－３の各々で暗号化している。

【００３７】図３に説明を戻すと、次に、集計サーバ４－１～４－３では、ディジタル署名に基づいて認証サーバ署名を検証し、認証サーバ２により認証された投票情報であるか否かをチェックする（ステップＳ１６）。次に、集計サーバ４－１～４－３は、例えばその時点における日時分秒ミリ秒マイクロ秒のデータのハッシュ値をとることで識別子を生成し（ステップＳ１７）、投票情報に付加して集計データベース５－１～５－３へ格納するとともに、投票情報に基づいて投票を集計する。開票終了後、集計サーバ４－１～４－３の各々において、それぞれ独立に集票・集計した投票結果を照合し、不一致が見つかった場合には、多数決で正解値を決める。

【００３８】

【発明の効果】以上説明したように、本発明によれば、ネットワークに接続された投票端末から投票者が投票し、該投票された投票内容を、前記ネットワークに接続された認証装置により認証し、前記認証された投票内容を暗号化して、前記ネットワークを介して、前記認証装置に接続されている集計装置に送信し、前記集計装置によって前記暗号化投票内容を復号して投票内容を取得し、該投票内容に基づいて候補者の得票を集計するようにしたので、人手の削減、開票スペースの縮小、無効票や疑問票の根絶、集計ミスの防止を実現することができるという利点が得られる。

【図面の簡単な説明】

【図１】　本発明の実施形態による電子投票システムの構成を示すブロック図である。

【図２】　本実施形態による投票者のＩＤ、パスワードの構成を示す概念図である。

【図３】　本発明の実施形態による電子投票システムの動作を説明するためのフローチャートである。

【図４】　認証サーバからディジタル署名を得る過程を示すフローチャートである。

【図５】　投票端末での密封、認証サーバでの開封、集計サーバでの開封の様子を示す概念図である。

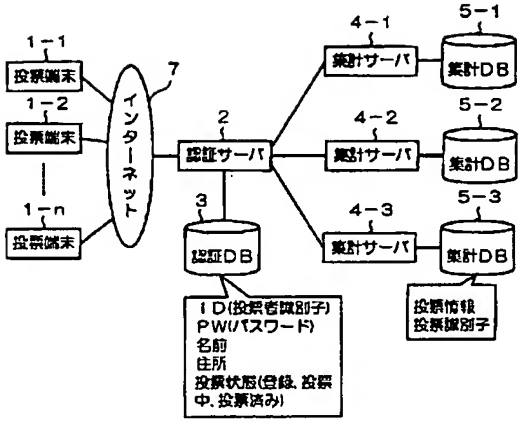
【図６】　投票端末での密封の詳細な様子を示す概念図である。

【図７】　認証サーバでおよび集計サーバでの開封の詳細な様子を示す概念図である。

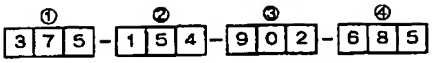
【符号の説明】

１－１～１－ｎ　投票端末
２　認証サーバ（認証装置）
３　認証データベース
４－１～４－３　集計サーバ（集計装置）
５－１～５－３　集計データベース
７　インターネット

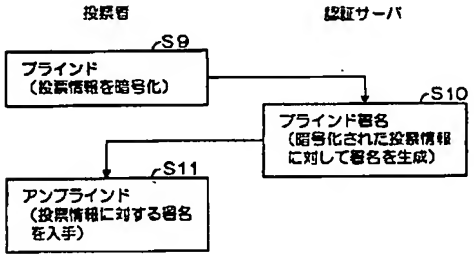
【図１】


1－1
投票端末
1－2
投票端末
1－n
投票端末
インターネット
7
2
認証サーバ
3
認証DB
ＩＤ(投票者識別子)
PW(パスワード)
名前
住所
投票状態(登録,投票中,投票済み)
4－1
集計サーバ
4－2
集計サーバ
4－3
集計サーバ
5－1
集計DB
5－2
集計DB
5－3
集計DB
投票情報
投票識別子

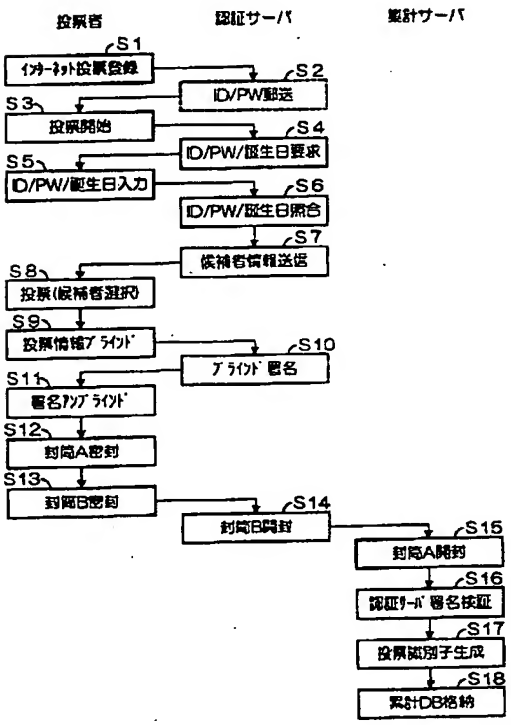
【図２】


①
②
③
④
3 7 5 - 1 5 4 - 9 0 2 - 6 8 5

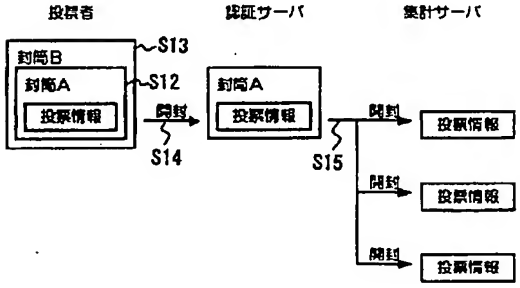
【図４】


投票者
認証サーバ
S9
ブラインド
（投票情報を暗号化）
S10
ブラインド署名
（暗号化された投票情報に対して署名を生成）
S11
アンブラインド
（投票情報に対する署名を入手）

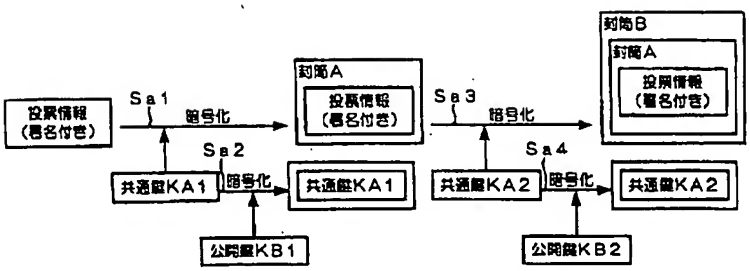
【図３】


投票者
認証サーバ
集計サーバ
S1
インターネット投票登録
S2
ID/PW郵送
S3
投票開始
S4
ID/PW/誕生日要求
S5
ID/PW/誕生日入力
S6
ID/PW/誕生日照合
S7
候補者情報送信
S8
投票(候補者選択)
S9
投票情報ブラインド
S10
ブラインド署名
S11
署名アンブラインド
S12
封筒A密封
S13
封筒B密封
S14
封筒B開封
S15
封筒A開封
S16
認証サーバ署名検証
S17
投票識別子生成
S18
集計DB格納

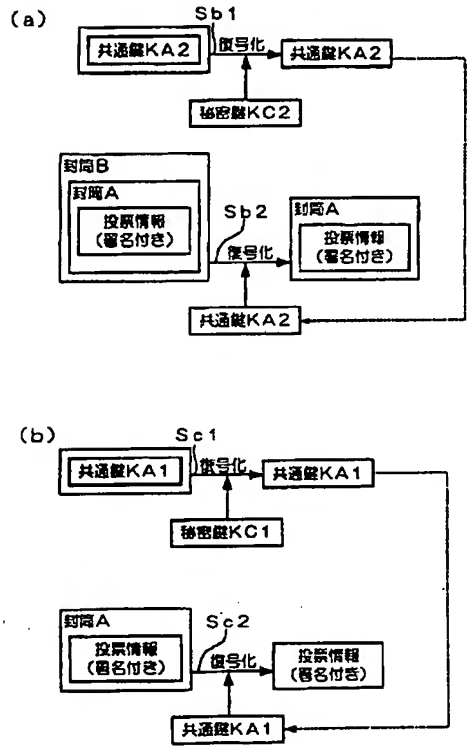
【図５】


投票者
認証サーバ
集計サーバ
封筒B
封筒A
投票情報
S13
S12
開封
S14
封筒A
投票情報
S15
開封
投票情報
開封
投票情報
開封
投票情報

【図６】



【図７】



フロントページの続き

(51)Int.Cl.'		識別記号	FI		テーマコード（参考）
G09C	1/00	660	G09C	1/00	660Z
H04L	9/32		H04L	9/00	673A
					675B

(19) Japan Patent Office (JP)
(12) **Japanese Unexamined Patent Application Publication (A)**

(11) Japanese Unexamined Patent Application Publication Number
2002–259621
(P2002-259621A)
(43) Publication date 13 September 2002 (2002.9.13)

(51) Int. Cl.[7]	Identification symbols	FI		Subject codes (reference)
G 06 F 17/60	148	G 06 F 17/60	148	5J104
	154		154	
	502		502	
	510		510	
	512		512	

Request for examination: Not filed Number of Claims: 11 OL (8 pages total) Continued on last page

(21) Application No. 2001–52429 (P2001–52429)

(22) Filing date 27 February 2001 (2001.2.27)

(71) Applicant 000102739
NTT Advanced Technology Corp.
1-1 Nishi Shinjuku 2-chome, Shinjuku-ku, Tokyo

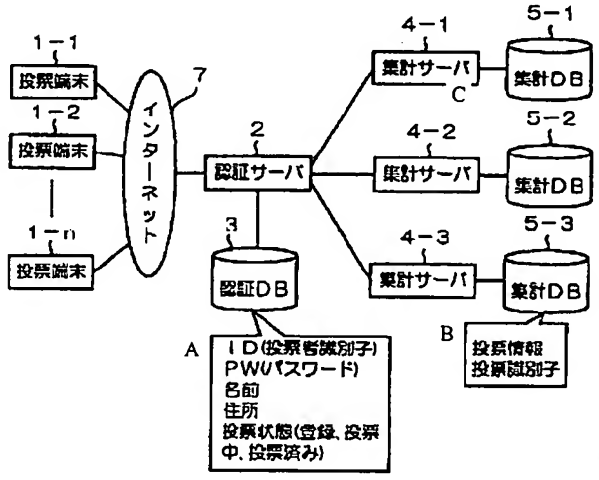
(72) Inventor Tanaka, Toshikiyo
c/o NTT Advanced Technology Corp.
1-1 Nishi Shinjuku 2-chome, Shinjuku-ku, Tokyo

(74) Agent 100064908
Patent Attorney Shiga, Masatake

F terms (reference) 5J104 AA07 AA09 AA16 EA06 EA19
KA01 LA08 MA01 NA05 NA35
NA41 PA17

(54) {Title of invention} Electronic voting system and electronic voting method

(57) {Abstract}
{Problem} To achieve reduction in amount of labor, reduction of ballot opening space, elimination of invalid ballots and questionable ballots, and prevention of counting errors.
{Solution} Voters vote at voting terminals 1–1 through 1–n by using a touch panel. An authentication server 2 generates a blind signature for the vote information to authenticate the voter. Voting terminals 1–1 through 1–n seal the vote information in a double electronic envelope by means of encryption techniques and send it over the internet 7 to the authentication server 2. The authentication server 2 unseals the outer envelope and sends the result to three counting servers 4–1 through 4–3. Each of the counting servers 4–1 through 4–3 unseals the inner envelope and performs counting based on the vote content. After opening of ballots is completed, the counting servers 4–1 through 4–3 compare the collected and counted results of voting, and in case a discrepancy is discovered, determine the correct value by majority decision.



1–1, 1–2, 1–n: Voting terminal
2: Authentication server
3: Authentication DB
4–1, 4–2, 4–3: Counting server
5–1, 5–2, 5–3: Counting DB
7: Internet
A: ID (voter identifier)
PW (password)
Name
Address
Voting status (registered, voting in progress, voting completed)
B: Vote information
Vote identifier

{Scope of patent Claims}

{Claim 1} An electronic voting system distinguished in that it comprises:

a voting terminal connected to a network, which encrypts the content of votes cast by voters for candidates and generates encrypted vote content;

an authentication device which authenticates said voters at said voting terminal via said network; and

a counting device which decrypts the encrypted vote content obtained from said voting terminal via said authentication device to acquire the vote content, and counts the votes obtained by candidates based on said vote content.

{Claim 2} An electronic voting system as described in Claim 1, distinguished in that:

said voting terminal comprises

a first encryption means which encrypts the content of the vote cast by the voter to generate a first encrypted vote content; and

a second encryption means which encrypts the first encrypted vote content encrypted by said first encryption means to generated a second encrypted vote content;

said authentication device comprises:

a first decryption means which decrypts the second encrypted vote content encrypted by said second encryption means of said voting terminal to obtain said first encrypted vote content;

and said counting device comprises:

a second decryption means which decrypts the first encrypted vote content decrypted by said first decryption means of said authentication device to obtain said vote content.

{Claim 3} An electronic voting system as described in Claim 2, distinguished in that said first encryption means

encrypts the content of the vote cast by the voter using a first common key and encrypts said first common key using a first public key of said counting device;

said second encryption means

encrypts said first encrypted vote content using a second common key and encrypts said second common key using a second public key of said authentication device;

said first decryption means comprises a second common key decryption means which decrypts the encrypted second common key using a second secret key corresponding to said second public key to obtain said second common key, and a second encrypted vote content decryption means which decrypts said second encrypted vote content using the decrypted second common key to obtain said first encrypted vote content;

and said second decryption means comprises a first common key decryption means which decrypts the encrypted first common key using a first secret key corresponding to said first public key to obtain said first common key, and a first encrypted vote content decryption means which decrypts said first encrypted vote content using the decrypted first common key to obtain said vote content.

{Claim 4} An electronic voting system as described in any of Claims 1 through 3, distinguished in that

said authentication device comprises:

a blind signing means which generates a blind signature for the vote content encrypted by said voting terminal to authenticate the legitimacy of the voter;

and said voting terminal comprises:

a third encryption means which encrypts the content of the vote for candidates selected by the voter and transmits it to said authentication device; and

a signature acquisition means which acquires signature information from the blind signature generated by the blind signing means of said authentication device.

{Claim 5} An electronic voting system as described in any of Claims 1 through 4, distinguished in that:

said counting device comprises:

an identification information generating means which generates identification information for said vote content; and

a storage means which stores said vote content together with said identification information.

{Claim 6} An electronic voting system as described in any of Claims 3 through 5, distinguished in that said first public key and first secret key as well as said second public key and second secret key are each generated and managed within an IC card that can be installed in and removed from said authentication device or said counting device and which is protected so as to prevent external leakage of information.

{Claim 7} An electronic voting method distinguished in that:

a voter casts a vote from a voting terminal connected to a network;

said cast vote content is encrypted and transmitted to an authentication device connected to said network;

said authentication device performs authentication of the voter, and if he was authenticated, transmits said encrypted content to said counting device;

said encrypted vote content is decrypted by said counting device to obtain the vote content; and

the votes obtained by candidates are counted based on said vote content.

{Claim 8} An electronic voting method as described in Claim 7, distinguished in that:

said voting terminal encrypts said vote content to generate encrypted vote content;

said authentication device generates a blind signature for the encrypted vote content encrypted by said voting terminal; and

said voting terminal obtains signature information from said blind signature.

{Claim 9} An electronic voting method as described in Claim 7, distinguished in that:

in the encryption of said vote content,

the content of the vote cast by said voter is encrypted using a first common key to generate said first encrypted vote content;

said first common key is encrypted using a first public key of said counting device;

said first encrypted vote content is encrypted using a second common key to generated second encrypted vote content;

said second common key is encrypted using a second public key of said authentication device;

and in the decryption of said encrypted vote content,

said encrypted second common key is decrypted using a second secret key corresponding to said second public key to obtain said second common key;

said second encrypted vote content is decrypted using said decrypted second common key to obtain said first encrypted vote content;

said encrypted first common key is decrypted using a first secret key corresponding to said first public key to obtain said first common key; and

said first encrypted vote content is decrypted using said decrypted first common key to obtain the vote content.

{Claim 10} An electronic voting method as described in any of Claims 7 through 9, distinguished in that identification information is generated for said vote content, and said vote content is stored together with said identification information.

{Claim 11} An electronic voting method as described in any of Claims 7 through 10, distinguished in that said first public key and first secret key as well as said second public key and second secret key are each generated and managed within an IC card that can be installed in and removed from the authentication device or counting device and which is protected so as to prevent external leakage of information.

{Detailed description of the invention}

{0001}

{Technical field of the invention} The present invention relates to electronic voting systems and electronic voting method suitably used in voting in national political elections, regional elections and the like.

{0002}

{Prior art} In the prior art, voting in national political elections, regional elections and the like has been carried out by having eligible voters write the names of candidates on ballots at polling places, gathering said ballots, and confirming and counting the candidate names written on the ballots, one by one, with much labor.

{0003}

{Problem to be solved by the invention} However, in the aforementioned prior art, large amounts of labor and ballot opening space is required. Furthermore, since the voter name is written by hand by the voter, invalid votes and questionable votes due to clerical errors cannot be eliminated. Furthermore, due to the visual confirmation by people, there was the problem that counting errors would also occur.

{0004} This invention was made in view of the above situation, and has the objective of providing an electronic voting system and electronic voting method capable of achieving reduction in amount of labor, reduction of ballot opening space, elimination of invalid ballots and questionable ballots, and prevention of counting errors.

{0005}

{Means of solving the problem} To resolve the aforesaid problems, the invention described in Claim 1 is distinguished in that it comprises a voting terminal connected to a network, which encrypts the content of votes cast by voters for candidates and generates encrypted vote content; an authentication device which authenticates said voters at said voting terminal via said network; and a counting device which decrypts the encrypted vote content obtained from said voting terminal via said authentication device to acquire the vote content, and counts the votes obtained by candidates based on said vote content.

{0006} Furthermore, the invention described in Claim 2 is distinguished in that, in the electronic voting system described in Claim 1, said voting terminal comprises: a first encryption means which encrypts the content of the vote cast by the voter to generate a first encrypted vote content, and a second encryption means which encrypts the first encrypted vote content encrypted by said first encryption means to generated a second encrypted vote content; said authentication device comprises a first decryption means which decrypts the second encrypted vote content encrypted by said second encryption means of said voting terminal to obtain said first encrypted vote content; and said counting device comprises a second decryption means which decrypts the first encrypted vote content decrypted by said first decryption means of said authentication device to obtain said vote content.

{0007} Furthermore, the invention described in Claim 3 is distinguished in that, in the electronic voting method system described in Claim 2, said first encryption means encrypts the content of the vote cast by the voter using a first common key and encrypts said first common key using a first public key of said counting device; said second encryption means encrypts said first encrypted vote content using a second common key and encrypts said second common key using a second public key of said authentication device; said first decryption means comprises: a second common key decryption means which decrypts the encrypted second common key using a second secret key corresponding to said second public key to obtain said second common key, and a second encrypted vote content decryption means which decrypts said second encrypted vote content using the decrypted second common key to obtain said first encrypted vote content; and said second decryption means comprises: a first common key decryption means which decrypts the encrypted first common key using a first secret key corresponding to said first public key to obtain said first common key, and a first encrypted vote content decryption means which decrypts said first encrypted vote content using the decrypted first common key to obtain said vote content.

{0008} Furthermore, the invention described in Claim 4 is distinguished in that, in the electronic voting system as described in any of Claims 1 through 3, said authentication device comprises a blind signing means which generates a blind signature for the vote content encrypted by said voting terminal to authenticate the legitimacy of the voter; and said voting terminal comprises a third encryption means which encrypts the content of the vote for candidates selected by the voter and transmits it to said authentication device, and a signature acquisition means which acquires signature information from the blind signature generated by the blind signing means of said authentication device.

{0009} Furthermore, the invention described in Claim 5 is distinguished in that, in the electronic voting system as described in any of Claims 1 through 4, said counting device comprises an identification information generating means which generates identification information for said vote content, and a storage means which stores said vote content together with said identification information.

{0010} Furthermore, the invention described in Claim 6 is distinguished in that, in the electronic voting system as described in

any of Claims 3 through 5, said first public key and first secret key as well as said second public key and second secret key are each generated and managed within an IC card that can be installed in and removed from said authentication device or said counting device and which is protected so as to prevent external leakage of information.

{0011} To resolve the aforementioned problems, the invention described in Claim 7 is distinguished in that a voter casts a vote from a voting terminal connected to a network; said cast vote content is encrypted and transmitted to an authentication device connected to said network; said authentication device performs authentication of the voter, and if he was authenticated, transmits said encrypted content to said counting device; said encrypted vote content is decrypted by said counting device to obtain the vote content; and the votes obtained by candidates are counted based on said vote content.

{0012} Furthermore, the invention described in Claim 8 is distinguished in that, in the electronic voting method as described in Claim 7, said voting terminal encrypts said vote content to generate encrypted vote content; said authentication device generates a blind signature for the encrypted vote content encrypted by said voting terminal; and said voting terminal obtains signature information from said blind signature.

{0013} Furthermore, the invention described in Claim 9 is distinguished in that, in the electronic voting method as described in Claim 7, in the encryption of said vote content, the content of the vote cast by said voter is encrypted using a first common key to generate said first encrypted vote content; said first common key is encrypted using a first public key of said counting device; said first encrypted vote content is encrypted using a second common key to generated second encrypted vote content; said second common key is encrypted using a second public key of said authentication device; and in the decryption of said encrypted vote content, said encrypted second common key is decrypted using a second secret key corresponding to said second public key to obtain said second common key; said second encrypted vote content is decrypted using said decrypted second common key to obtain said first encrypted vote content; said encrypted first common key is decrypted using a first secret key corresponding to said first public key to obtain said first common key; and said first encrypted vote content is decrypted using said decrypted first common key to obtain the vote content.

{0014} Furthermore, the invention described in Claim 10 is distinguished in that, in the electronic voting method as described in any of Claims 7 through 9, identification information is generated for said vote content, and said vote content is stored together with said identification information.

{0015} Furthermore, the invention described in Claim 11 is distinguished in that, in the electronic voting method as described in any of Claims 7 through 10, said first public key and first secret key as well as said second public key and second secret key are each generated and managed within an IC card that can be installed in and removed from the authentication device or counting device and which is protected so as to prevent external leakage of information.

{0016} In this invention, a voter casts a vote from a voting terminal connected to a network; said cast vote content is authenticated by an authentication device connected to said network; said authenticated vote content is encrypted and transmitted to a counting device connected to said authentication device; said encrypted vote content is decrypted by said counting device to obtain the vote content; and the votes obtained by candidates are counted based on said vote content. Thus, it becomes possible to achieve reduction in amount of labor, reduction of ballot opening space, elimination of invalid ballots and questionable ballots, and prevention of counting errors.

{0017}

{Modes of embodiment of the invention} Below, modes of embodiment of the present invention are described using the drawings.

A. Constitution of the mode of embodiment

Figure 1 is a block diagram showing the constitution of an electronic voting system according to a mode of embodiment of the present invention. In Figure 1, voting terminals 1–1, 1–2, ..., 1–n are terminals installed at a polling place, and are made up of personal computers and the like. Said voting terminals 1–1 through 1–n are connected to the internet 7. Multiple (n) voting terminals 1–1 through 1–n are installed at a single polling place, the number of terminals installed being determined in accordance with the number of eligible voters voting at the polling place.

{0018} Said voting terminals 1–1 through 1–n have the function of encrypting candidate information, the function of decrypting (unblinding) digital signatures generated by the authentication server 2 described below, as well as the function of performing double encryption on candidate information and digital signatures, and the like. These functions (operations) will be discussed below.

{0019} A voter enters an ID (voter identifier) and password for authenticating the voter, as well as candidates and the like, by touching numerical buttons on the touch panel of the voting terminals 1–1 through 1–n. The ID and password are for instance divided into groups of three columns, and each group is numbered. In consideration of elderly voters and the like, the ID and password are preferably made up of numerals only, so as to reduce misreading or input errors.

{0020} The voting terminals 1–1 through 1–n may also be installed at a voter's home, in which case specific voting software needs to be installed in advance.

{0021} The authentication server 2 requests said ID, password, birth date, etc. from the voting terminals 1–1 through 1–n via the internet 7, and verifies those pieces of information to authenticate the voter. Furthermore, the authentication server 2 transmits candidate information (name, party, face photograph) to the voting terminals 1–1 through 1–n via the internet 7, and issues a digital signature (blind signature) for (encrypted) vote information from the voting terminals 1–1 through 1–n. Moreover, the authentication server 2 transmits encrypted vote information from the voting terminals 1–1 through 1–n to three

counting servers 4–1, 4–2 and 4–3, which are described below. Moreover, the authentication server 2 comprises an authentication database for performing voter authentication, managing voting status, etc. Said authentication database 3 stores each voter's ID, password, name, address and voting status (registered, voting in progress, voting completed).

{0022} The counting servers 4–1 through 4–3 consist of three physically separated servers having the same functions. The counting servers 4–1 through 4–3 each independently perform vote collection and counting. More specifically, the counting servers 4–1 through 4–3 verify the digital signature made by the authentication server 2 for vote information from the authentication server 2, generate and append a vote identifier thereto, and store it in counting databases 5–1, 5–2 and 5–3. The results of counting by the respective counting servers 4–1 through 4–3 are compared to each other, and if a discrepancy is discovered, the correct value is determined by majority decision.

{0023} The aforementioned authentication server 2 and counting servers 4–1 through 4–3 are made to perform encryption, decryption and digital signing of vote information; the generation of secret keys used in said encryption, decryption and digital signing, as well as decryption and signature generation, are performed on a storage medium such as an IC card. The secret key is protected so that it cannot be read out from the IC card. Thus, since backups against loss or the like cannot be made, as many signings and encryptions are performed as the number of secret keys (2 in this example; 3 in case of counting servers) to provide redundancy.

{0024} B. Operation of the mode of embodiment

Next, operation of the present mode of embodiment is described in detail with reference to the flow chart shown in Figure 3. Here, Figure 4 is a flow chart showing the process of obtaining a digital signature from the authentication server. Furthermore, Figure 5 is a conceptual drawing which shows the situation of envelope sealing at said voting terminals, unsealing at the authentication server and unsealing at the counting servers.

{0025} A voter accesses the authentication server in advance via the internet from a terminal at his home and registers personal information (name, address, etc.) from an election administration Web screen presented by the authentication server (Step S1). The authentication server 2 mails a sealed postcard (voting card) with the ID (voter identifier) and PW (password) for the registered voter inscribed thereon to the voter's home (Step S2). Since there are eligible voters who may not have a terminal at home, sealed postcards (voting cards) may also be automatically mailed to the homes of eligible voters from the authentication server 2 (competent government office), as per the current practice.

{0026} Next, on polling day, voters cast votes from the terminals at their home. Voters who do not have a terminal at home take the voting card mailed to their home and go to a polling place, and cast votes from terminals at the polling place. Voters commence voting from a voting terminal 1–i (i = 1 ~ n) installed at home or at a polling place (Step S3).

{0027} The authentication server 2 requests input of ID, password and birth date from said voting terminal 1–i via the internet 7 (Step S4). The voter inputs the ID, password and birth date (MMDD) printed on the sealed postcard mailed to his home via the touch panel of the voting terminal 1–i (Step S5). The ID and password are transmitted via the internet 7 to the authentication server 2.

{0028} The authentication server 2 compares the ID, password and birth date input from said voting terminal 1–i against information in the authentication database 3 to check if this is a proper voter, i.e. an eligible voter, and that this is not a case of duplicate voting (Step S6). If the voter was authenticated as being legitimate, the authentication server 2 transmits candidate information (name, party, face photograph, etc.) via the internet 7 to said voting terminal 1–i (Step S7). If the voter was not authenticated as legitimate, that fact is displayed on the voting terminal 1–i and processing for the voter in question is discontinued.

{0029} The voter confirms the candidate information displayed on the voting terminal 1–i and selects (votes for) candidates (Step S8). The voting terminal 1–i, as shown in Figure 4, blinds (encrypts) the selected candidate information (hereinafter, vote information) and transmits it via the internet 7 to the authentication server 2 (Step S9). The authentication server 2, as shown in Figure 4, generates a digital signature (blind signature) for said encrypted vote information and transmits it via the internet 7 to the voting terminal 1–i (Step S10). The voting terminal 1–i, as shown in Figure 4, unblinds (decrypts) said blind signature to obtain a digital signature (Step S11). In this way, by using a blind signature, the authentication server 2 can ascertain the voter but cannot find out the vote content (guarantee of anonymity). Furthermore, the authentication server authenticates the voter's identity, that the vote content was produced by that voter, and that the vote was not cast in duplicate.

{0030} Next, an example of the blind signing scheme is described. It is assumed that d is the authentication server's secret key, e and n are the public keys, and m is the vote information. Furthermore, the computational operations below are based on the residue of n. The voting terminal generates a random number r, and sends the product of r to the power of e and m to the authentication server as x. The authentication server takes x to the power of d and sends it to the voting terminal as y. This y is the blind signature. The voting terminal divides y by r. Since d = 1/e, the results of the division will be m to the power of d, which is the signature for m proper.

{0031} Next, the voting terminal 1–i, as shown in Figure 5, seals said vote information (including digital signature) in an envelope A (Step S12), and then again seals it in an envelope

B (Step S13) and transmits it via the internet 7 to the authentication server 2. The authentication server 2, as shown in Figure 5, unseals only the outer envelope B (Step S14) and transmits the result to the counting servers 4–1 through 4–3. The counting servers 4–1 through 4–3, as shown in Figure 5, unseal the envelope A (Step S15) and obtain the original vote information (including digital signature).

{0032} Below, the sealing of the envelope at said voting terminals 1–1 through 1–n, the unsealing at authentication server 2 and unsealing at the counting servers 4–1 through 4–3 is described in more detail. Here, Figure 6 is a conceptual drawing which shows the detailed situation of sealing at said voting terminals. Furthermore, Figure 7 is a conceptual drawing which shows the detailed situation of unsealing at said authentication server and counting servers.

{0033} At the voting terminals 1–1 through 1–n, as shown in Figure 6, the aforementioned vote information (including digital signature) is encrypted with a common key KA1 (Step Sa1), thereby sealing it in envelope A, and then said common key KA1 is encrypted with a public key KB1 published by the counting servers 4–i (i = 1, 2, 3) (Step Sa2). Next, the encrypted vote information (envelope A) is further encrypted with common key KA2 (Step Sa3) to seal it in envelope B, after which said common key KA2 is encrypted with a public key KB2 published by the authentication server 2 (Step Sa4). The vote information is thereby sealed (encrypted) doubly, in envelope A (inner) and envelope B (outer). Said double encrypted vote information is transmitted via the internet 7 to the authentication server 2.

{0034} At the authentication server 2, as shown in Figure 7(a), the encrypted common key KA2 is decrypted with the secret key KC2 corresponding to said public key KB2 to obtain said common key KA2 (Step Sb1) and said double encrypted vote information (inner: envelope A; outer: envelope B) is decrypted with said common key KA2 to unseal the outer envelope B (Step Sb2). The vote information sealed in envelope A is then transmitted to the counting servers 4–1 through 4–3.

{0035} At the counting server 4–i (i = 1, 2, 3), as shown in Figure 7(b), the encrypted common key KA1 is decrypted by the secret key KC1 corresponding to said public key KB1 to obtain the common key KA1 (Step Sc1), and said vote information (envelope A) is decrypted with said common key KA1 to unseal envelope A (Step Sc2). At this point, the counting server 4–i obtains the original vote information (including digital signature).

{0036} In the foregoing description, the present mode of embodiment employs three counting servers 4–1 through 4–3, so in actuality, the counting servers would each generate their respective secret key KC1–1, KC1–2 or KC1–3 and the public key KB1–1, KB1–2 or KB1–3 corresponding to said secret key. Then the voting terminal 1–i, when sealing the vote information in envelope A, would encrypt the common key KA1 with each of said public keys KB1–1, KB1–2 and KB1–3.

{0037} Returning to Figure 3, next, the counting servers 4–1 through 4–3 verify the authentication server signature based on the digital signature to check whether or not the vote information has been authenticated by the authentication server 2 (Step S16). Next, the counting servers 4–1 through 4–3 generate an identifier, for instance by taking the current date, hour, minute, second, millisecond and microsecond data as a hash value (Step S17), append it to the vote information and store it in the counting databases 5–1 through 5–3, and also count the vote based on the vote information. After completion of ballot opening, the voting results from the ballots collected and counted independently at each of the counting servers 4–1 through 4–3 are compared, and if a discrepancy is discovered, the correct value is determined by majority decision.

{0038}

{Effect of the invention} As described above, according to the present invention, voters cast votes from voting terminals connected to a network, said cast vote content is authenticated by an authentication device connected to said network, said authenticated vote content is encrypted and transmitted via said network to a counting device connected to said authentication device, said encrypted vote content is decrypted by said counting device to obtain the vote content, and the votes obtained by candidates are counted based on said vote content, thereby providing the advantages of allowing one to achieve reduction in amount of labor, reduction of ballot opening space, elimination of invalid ballots and questionable ballots, and prevention of counting errors.

{Brief description of the drawings}

{Figure 1} A block diagram showing the constitution of an electronic voting system according to a mode of embodiment of the present invention.

{Figure 2} A conceptual diagram showing the constitution of the voter ID and password according to the present mode of embodiment.

{Figure 3} A flow chart explaining the operation of an electronic voting system according to a mode of embodiment of the present invention.

{Figure 4} A flow chart showing the process of obtaining a digital signature from the authentication server.

{Figure 5} A conceptual drawing showing the situation of envelope sealing at voting terminals, unsealing at the authentication server, and unsealing at the counting servers.

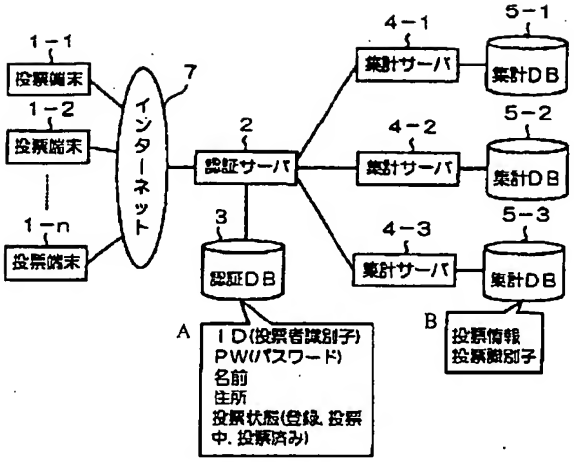
{Figure 6} A conceptual drawing which shows the detailed situation of envelope sealing at the voting terminals.

{Figure 7} A conceptual drawing which shows the detailed situation of envelope unsealing at the authentication server and counting servers.

{Description of captions}

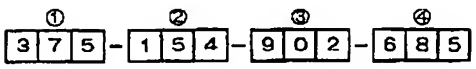
1–1 ~ 1–n Voting terminal
2 Authentication server (authentication device)
3 Authenticate database
4–1 ~ 4–3 Counting server (counting device)
5–1 ~ 5–3 Counting database
7 Internet

{Figure 1}

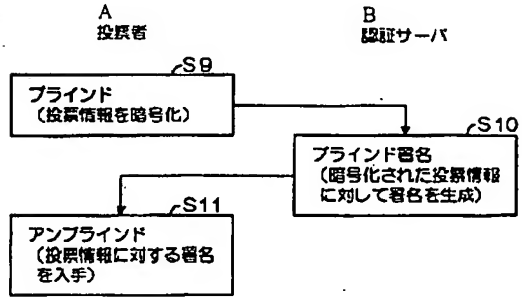


1-1, 1-2, 1-n: Voting terminal
2: Authentication server
3: Authentication DB
4--1, 4-2, 4-3: Counting server
5-1, 5-2, 5--3: Counting DB
7: Internet
A: ID (voter identifier)
PW (password)
Name
Address
Voting status (registered, voting in progress, voting completed)
B: Vote information
Vote identifier

{Figure 2}

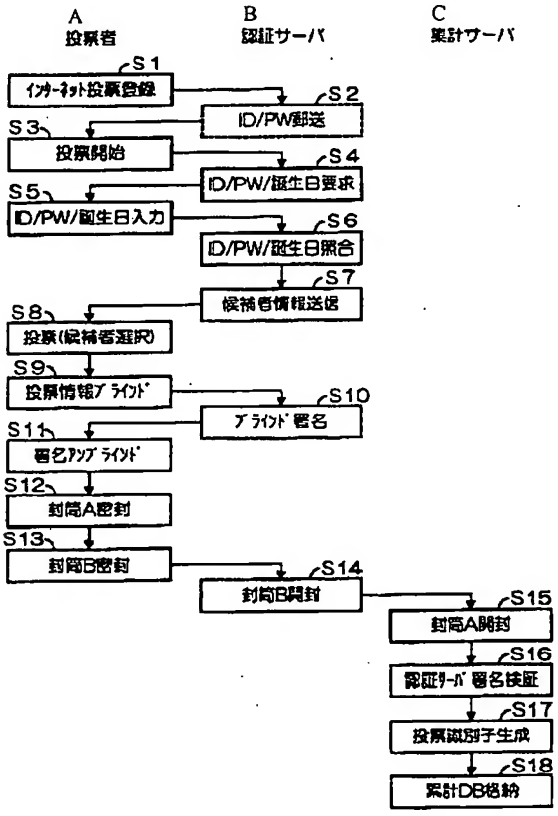


{Figure 4}



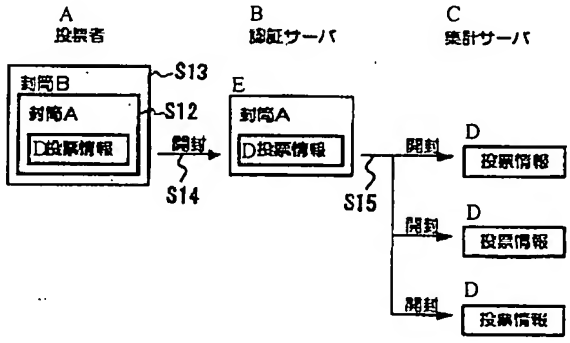
A: Voter
B: Authentication server
S9: Blinding (encryption of vote information)
S10: Blind signing (generation of signature for encrypted vote information)
S11: Unblinding (obtaining signature for vote information)

{Figure 3}



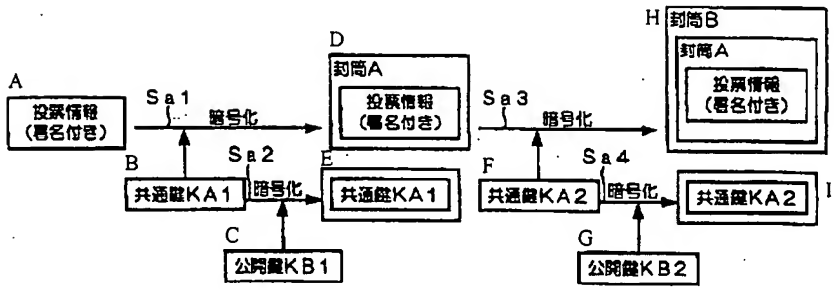
A: Voter
B: Authentication server
C: Counting server
S1: Internet voting registration
S2: ID/PW mailing
S3: Start of voting
S4: ID/PW/birth date request
S5: ID/PW/birth date input
S6: ID/PW/birth date verification
S7: Candidate information transmission
S8: Voting (candidate selection)
S9: Vote information blinding
S10: Blind signing
S11: Signature unblinding
S12: Envelope A sealing
S13: Envelope B sealing
S14: Envelope B unsealing
S15: Envelope A unsealing
S16: Authentication server signature verification
S17: Vote identifier generation
S18: Storage in cumulative DB

{Figure 5}



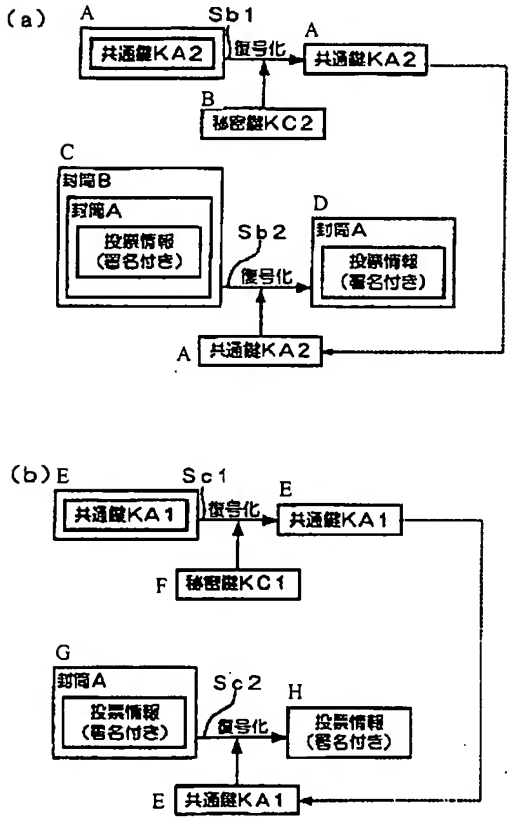
A: Voter
B: Authentication server
C: Counting server
D: Vote information
E: Envelope A
S12: Envelope A
S13: Envelope B
S14, S15: Unsealing

{Figure 6}



A: Vote information (signed)
B: Common key KA1
C: Public key KB1
D: Envelope A
Vote information (signed)
E: Public key KA1
F: Common key KA2
G: Public key KB2
H: Envelope B
Envelope A
Vote information (signed)
I: Common key KA2
Sa1, Sa2, Sa3, Sa4: Encryption

{Figure 7}



A: Common key KA2
B: Secret key KC2
C: Envelope B
Envelope A
Vote information (signed)
D: Envelope A
Vote information (signed)
E: Common key KA1
F: Secret key KC1
G: Envelope A
Vote information (signed)
H: Vote information (signed)
Sb1, Sb2, Sc1, Sc2: Decryption

Continuation of front page

(51) Int. Cl.[7]		Identification symbols	FI		Subject codes (reference)
G 09 C	1/00	660	G 09 C	1/00	660Z
H 04 L	9/32		H 04 L	9/00	673A
					675B

JOB # 71514

Language Pairs		Client Contact	Ms. Anita Hogan	Industry	LEGAL
Japanes	English (USA)	Billing Contact	Ms. Anita Hogan	Class ID	ASIAN DEPT.
...	...	Company	Foley & Lardner		
...	...	Address	Washington Harbour	Date Started?	Thursday, 12/05/02
...	...		3000 K Street, NW, St	Time Started?	9:00am
...	...		Washington, DC 20007		
...	...			Date Due	Friday, 12/06/02
...	...	Acct. Executive	BChristian	Time Due	4:00pm
...	...	PM/BMM	FIshikawa		
...	...	LMM	(none)		
...	...	DM	(unassigned)	Translator Word Ct.	
...	...				
...	...	Internal Trans	(none)	Software Word Ct.	

Interim Deadlines?
(Please include details here)

Special Instructions
Please include reference numbers in the translation and page break between each number. Do not put the reference # in a Header - just put at the top of each page. Please use a regular Foley translator. Budget is $0.14/wd.

Deliverables
MS Word 97 file

Delivery Method
emailed to jgabler & lsherfinski

Billing Description
Japanese into English translation requested 12/5/2002: Ref# 40405/340 & 16891/799

Production Project Description
Japanese into English translation requested 12/5/2002: Ref# 40405/340 & 16891/799

Print/DTP Checklist

All source files?	(Y/N)
Version	(Y/N)
Mac/PC?	(Y/N)
Fonts?	(Y/N)
EPS/Source Graphics?	(Y/N)
Output Resolution?	(Y/N)
PDF needed?	No

Notes

Total Budget	70.00
Word Count (AE)	500

Budget Breakdown below for **SINGLE LANGUAGE** jobs **ONLY**! For Multilingual, you must **consult the LP tabs** of toolkit to see **beyond the first language**!!!

LP1 ONLY!!!!!

Cost Category	Unit	Quantity	Total
TEP-M	0.14	500.00	70.00
...	0.00	0.00	0.00
...	0.00	0.00	0.00
...	0.00	0.00	0.00
...	0.00	0.00	0.00
...	0.00	0.00	0.00
		Total	70.00